CONGRUENCE

Definition: Let n be a fixed integer. Two integers a and b are said to be congruent modulo n, symbolized by

$$a \equiv b \ (mod\ n), \qquad a, b, n \in \mathbb{Z}$$

If n divides the difference $a - b$; that is provided that $a - b = kn$ for some integer k.

Example: $5 \equiv 25\ (mod\ 5)$; $a = 5, b = 25, n = 5\ (a, b, n \in \mathbb{Z})$

. If $5|(5 - 25)$, then $5 \equiv 25\ (mod\ 5)$

. $5|(5 - 25)$

$\Rightarrow \ 5| - 20 \quad \rightarrow \quad -20 = 5\,(-4), \ -4 \in \mathbb{Z}$

NOTE: $a \equiv b\ (mod\ n) \rightarrow \ n|(a - b)$ $\qquad$ $\exists\ x \in \mathbb{Z}$ such that

By definition of Congruence $\qquad$ By Definition of Divisibility

$$\boxed{\begin{array}{c} a - b = nx \\ a = nx = b \end{array}}$$

A. BASIC PROPERTIES OF CONGRUENCE

Let $a, b, c \in \mathbb{Z}$, then:

a) Reflexive Property: $a \equiv a\ (mod\ n)$ for some integer n.

Proof: Suppose $a, n \in \mathbb{Z}$. Since $n|0$ for any integer divides 0;

Therefore $0 = np$ for some integer p by ***definition of divisibility.***

So that:

- $0 = np$ $\qquad$ ***By definition of Divisibility***

$\Rightarrow \quad a - a = np$	***Rewrite* $\mathbf{0}$ *as* $\boldsymbol{a-a}$ *for any integer* $\boldsymbol{a}$**

Since $a - a = np$, therefore, $n|(a - a)$ by ***definition of divisibility.***

Thus,* $\boldsymbol{a \equiv a\ (mod\ n)}$ *by definition of congruence.

b) ***Symmetric Property:*** If $a \equiv b\ (mod\ n)$, then $b \equiv a\ (mod\ n)$.

Given: $\boldsymbol{a} \equiv b\ (mod\ n)$

Need to Show: $b \equiv a\ (mod\ n)$

Proof: $a \equiv b\ (mod\ n)$ yields to $n|(a - b)$ by ***definition of Congruence.***

Then, it follows that $a - b = nx, x \in \mathbb{Z}$ by ***definition of divisibility.***

Therefore,

• $a - b = nx$	***By definition of Divisibility***
$\Rightarrow \quad a + - b = nx$	***LHS: By definition of Subtraction***
$\Rightarrow \quad -1\ (a + -b) = -1\ (nx)$	***Multiply* $\mathbf{-1}$ *to both sides of the equation***
$\Rightarrow \quad -a + b = -nx$	***LHS: By Distributive Property for Multiplication over Addition*** ***RHS: Simplifying* $\boldsymbol{-1(nx)}$**
$\Rightarrow \quad b + - a = n\ (-x)$	***LHS: By Commutative Property for Addition*** ***RHS: Factor out* $\mathbf{n}$ *from* $\boldsymbol{-nx}$**

Since $-1, x \in \mathbb{Z}$, therefore, $-1.x = -x \in \mathbb{Z}$ by ***Closure Property for Multiplication.***

Let $y = -x$

$\Rightarrow\ b - a = ny$ ***LHS: By definition of Subtraction***

RHS: Rewriting $-x$ as y, where, $y \in \mathbb{Z}$.

$\Rightarrow\ n|(b-a)$ ***By Definition of Divisibility***

$\Rightarrow\ b \equiv a\ (mod\ n)$ ***By Definition of Congruence***

End of Proof.

c) ***Transitive Property*****:** If $a \equiv b\ (mod\ n)\ and\ b\ =\ c\ (mod\ n)$, then

$$a \equiv c\ (mod\ n).$$

Given: $a \equiv b(mod\ n);\ b \equiv c\ (mod\ n), a, b, c, n \in \mathbb{Z}$

Need to Show: $a \equiv c\ (mod\ n)$

Proof: $a\ \equiv b\ (mod\ n)$ means that $n|\ (a-b), and\ b \equiv c\ (mod\ n)$ means that $n|(b-c)$, both by ***definition of congruence***. Also, it follows that:

(1) $a - b = nx$, for some $x \in \mathbb{Z}$; and

(2) $b - 6\ = ny$, for some $y \in \mathbb{Z}$ both by ***definition of Divisibility.***

So that:

(3) $a - b\ =\ nx$

$\Rightarrow a - b + b = nx + b$ ***Add b to both sides of the equation***

$\Rightarrow a\ =\ nx + b$ ***Simplifying $-b + b$***

And

(4) $b - c = ny$

$\Rightarrow\ b - c + c =\ ny + c$ ***Add c to both sides of the equation***

$\Rightarrow\ b = ny + c$	***Simplifying*** $\boldsymbol{-c+c}$

Next, we use equations (3) and (4) to show that $a = c\ (mod\ n)$.

So that:

• $a = nx + b$	***From Equation(3)***
$\Rightarrow\ a = nx + (ny + c)$	***Substituting the value of b from Equation(4)***
$\Rightarrow\ a = (nx + ny) + c$	***By Associative Property for Addition***
$\Rightarrow\ a = n\,(x + y) + c$	$\boldsymbol{Factor\ out\ n\ from\ (nx+ny)}$

Since x, y, ∈ ℤ therefore, $x + y \in \mathbb{Z}$ by ***definition of Closure Property for Addition.***

$\Rightarrow\ a = nz + c$	***Let*** $\boldsymbol{x+y=z\in\mathbb{Z}}$
$\Rightarrow\ a + -c = nz + c + -c$	***Add*** $\boldsymbol{-c}$ ***to both sides of the equation***
$\Rightarrow\ a - c = nz$	***LHS: By definition of Subtraction*** ***RHS: Simplifying*** $\boldsymbol{c+-c}$
$\Rightarrow\ n\vert(a - c)$	***By Definition of Divisibility***
$\Rightarrow\ a \equiv c\ (mod\ n)$	***By Definition of Congruence***

A.1) ADDITIONAL PROPERTIES OF CONGRUENCE:

a) If $a \equiv b\ (mod\ n)$ and $d|n$, then $a \equiv b\ (mod\ d)$

Proof.

Given: $a \equiv b\ (mod\ n)$ and $d|n, a, b, d, n \in \mathbb{Z}$

Need to Show: $a \equiv b \ (mod\ d)$

- $a \equiv b \ (mod\ n)$

$\Rightarrow \quad n|(a - b)$ **By definition of Congruence**

(1) $\Rightarrow \quad a - b = np, \ p \in \mathbb{Z}$ **By definition of Divisibility**

and, we have:

$d|n$

(2) $\Rightarrow \quad n = dq\ , q \in \mathbb{Z}$ **By definition of Divisibility**

Now, using equations (1) and (2):

$a - b = np$ ***From Equation(1)***

$a - b = d\ (dq)\ p$ ***Substitute the value of $\mathbf{n}$ from Equation(2)***

$a - b = d\ (qp)\ p$ ***By Associative Property for Multiplication***

Since $q, p \in \mathbb{Z}$ therefore, $qp \in \mathbb{Z}$ by ***definition of Closure Property for Multiplication.***

Let $qp = r$

- $a - b = dr, r \in \mathbb{Z}$ ***Let $\boldsymbol{r = qp, r} \in \mathbb{Z}$***

$\Rightarrow \quad d|(a - b)$ ***By definition of Divisibility***

$\Rightarrow \quad a \equiv b\ (mod\ d)$ ***By definition of Congruence***

b) If $a \equiv b\ (mod\ n)$ and $c \equiv d\ (mod\ n)$, then:

i. $ax + cy \equiv (bx + dy)(mod\ n) \quad a, b, c, d, n, x, y \in \mathbb{Z}$

ii. $ac \equiv bd\ (mod\ n)$

For (b.i)

Proof.

Given: $a \equiv b\ (mod n)\ and\ c \equiv d(\ mod\ n)\ ;\ a, b, c, d, n\ \in \mathbb{Z}$

Need to Show: $(ax + cy) \equiv (bx + dy)\ (mod\ n)\ ;\ x, y \in \mathbb{Z}$

• $a \equiv b\ (mod\ n)$	***Given***
$\Rightarrow\ n \mid (a - b)$	***By definition of Congruence***
$\Rightarrow\ a - b = np, p\ \in \mathbb{Z}$	***By definition of Divisibility***
$\Rightarrow\ a - b + b = np + b$	***Add b to both sides of Equation***
(1) $\Rightarrow\ a = np + b$	***Simplifying*** $\boldsymbol{-b + b}$
• $c = d\ (mod\ n)$	***Given***
$\Rightarrow\ n \mid (c - d)$	***By definition of Congruence***
$\Rightarrow\ c - d =\ nq, q \in \mathbb{Z}$	***By definition of Divisibility***
$\Rightarrow\ c - d + d =\ nq + d$	***Add d both sides of Equation***
(2) $\Rightarrow\ c = nq + d$	***Simplifying*** $\boldsymbol{-d + d}$

So that:

• $ax +\ cy = (np\ +\ b)\ x\ +\ (nq + d)\ y$	***Substituting the values of a and c from Equations (1) and (2)***
$\Rightarrow\ ax + cy = (npx + bx)\ +\ (nqy + dy)$	***By Distributive Property for Multiplication over Addition***

Since $b, d, n, p, q, x, y \in \mathbb{Z}$, therefore, $npx, bx, nqy, dy \in \mathbb{Z}$, by ***Closure Property for Multiplication.***

$\Rightarrow \quad ax + cy = npx + (bx + nqy) + dy$	***By Associative Property for Addition***
$\Rightarrow \quad ax + cy = npx + (nqy + bx) + dy$	***By Commutative Property for Addition***
$\Rightarrow \quad ax + cy = (npx + nqy) + (bx + dy)$	***By Associative Property for Addition***
$\Rightarrow \quad ax + cy = n\,(px + qy) + (bx + dy)$	***Factor out $\boldsymbol{n}$ from $(\boldsymbol{npx + nqy})$***

Since $p, x, q, y \in \mathbb{Z}$, therefore $px, qy \in \mathbb{Z}$ by ***definition of Closure Property for Multiplication.*** Also, since. $px, qy, bx, dy \in \mathbb{Z}$, therefore $(px + qy), (bx + dy) \in \mathbb{Z}$ by ***Closure Property for Addition.***

$\Rightarrow \quad ax + cy = n\,(z) + (bx + dy)$	***Let $\boldsymbol{px + qy = z} \in \mathbb{Z}$***
$\Rightarrow \quad (ax + cy) + -(bx + dy)$ $= nz + (bx + dy) + -(bx + dy)$	***Add $-(\boldsymbol{bx + dy})$ to both sides of the Equation***
$\Rightarrow \quad (ax + cy) - (bx + dy) = nz$	***LHS: By definition of Subtraction*** ***RHS: Simplifying $(\boldsymbol{bx + dy}) + -(\boldsymbol{bx + dy})$***
$\Rightarrow \quad n \mid [(ax + cy) - (bx + dy)]$	***By definition of Divisibility***
$\Rightarrow \quad ax + cy \equiv (bx + dy) \pmod{n}$	***By definition of Congruence***

End of Proof.

For (b.ii)

Proof.

Given: $a \equiv b \ (mod\ n) \quad a, b, c, d, n \ \in \mathbb{Z}$

$c \equiv d \ (\ mod\ n)$

Need to Show: $ac \equiv bd \ (\ mod\ n)$

• $a \equiv b \ (mod\ n)$	***Given***
$\Rightarrow \ n\|(a-b)$	$\boldsymbol{By\ definition\ of\ Congruence}$
$\Rightarrow \ a - b = np,\ p \in \mathbb{Z}$	***By definition of Divisibility***
$\Rightarrow \ a - b + b \ = np + b$	***Add b to both sides of the Equation***
(1) $\Rightarrow \ a = np + b$	***LHS: Simplifying*** $\boldsymbol{-\ b + b}$
• $c \equiv d \ (\ mod\ n)$	***Given***
$\Rightarrow \ n\|(c-d)$	***By definition of Congruence***
$\Rightarrow \ c - d \ = nq, q \in \mathbb{Z}$	***By definition of Divisibility***
$\Rightarrow \ c \ - \ d + \ d = \ nq + d$	***Add*** $\boldsymbol{d}$ ***to both sides of the Equation***
(2) $\Rightarrow \ c = nq + d$	***LHS: Simplifying*** $\boldsymbol{-d + d}$

So that:

• $ac \equiv (np + b)(nq + d)$	***Substituting the values of a and c from Equations (1) and (2)***
$\Rightarrow \ ac \equiv (npnq + npd) + (bnq + bd)$	***By Distributive Property for Multiplication over Addition***

Since n, p, q, d, b $\in \mathbb{Z}$, therefore, $npnq, npd, bnq, bd \in \mathbb{Z}$ by ***Closure Property for Multiplication.*** Also, since $npnq, npd, bnq, bd \in \mathbb{Z}$, therefore, $(npnq + npd), (bnq + bd) \in \mathbb{Z}$ by ***Closure Property for Addition.***

$\Rightarrow \; ac = (npnq + npd + bnq) + bd$	***By Associative Property for Addition***
$\Rightarrow \; ac = n\,(npq + pd + bq) + bd$	***Factor out*** $\boldsymbol{n}$ ***from*** $(\boldsymbol{npnq} + \boldsymbol{npd} + \boldsymbol{bnq})$

Since $n, p, q, b, d \in \mathbb{Z}$, therefore, $npq, pd, bq \in \mathbb{Z}$. by ***Closure Property for Multiplication***. Also, since $, pd, bq \in \mathbb{Z}$, therefore $(npq + pd + bq) \in \mathbb{Z}$ by ***Closure Property for Addition***.

$\Rightarrow \; ac = nr + bd$	***Let*** $\boldsymbol{r} = \boldsymbol{npq} + \boldsymbol{pd} + \boldsymbol{bq},\; \boldsymbol{r} \in \mathbb{Z}$
$\Rightarrow \; ac + -bd = nr + bd + -bd$	***Add*** $\boldsymbol{-bd}$ ***to both sides of Equation***
$\Rightarrow \; ac - bd = nr$	***LHS: By definition of Subtraction*** ***RHS: Simplifying*** $\boldsymbol{bd} + \boldsymbol{-bd}$
$\Rightarrow \; n \mid (ac - bd)$	***By definition of Divisibility***
$\Rightarrow \; ac \equiv bd \pmod{n}$	***By definition of Congruence***

End of Proof.

c) If $a \equiv b \pmod{n}$, then:

   i. $a + c \equiv b + c \pmod{n}$
   ii. $ac \equiv bc \pmod{n}$
   iii. $a^k \equiv b^k \pmod{n}$

For (c.i)

Proof.

Given: $a \equiv b\ (mod\ n)\quad a, b, n \in \mathbb{Z}$

Need to Show: $a + c \equiv b + c\ (mod\ n)$

Suppose $a, b, n\ \in \mathbb{Z}$, where $a\ \equiv\ b\ (mod\ n)$. Then it follows that:

• a = b (mod n)	***Given***
⇒ $n|(a - b)$	***By definition of Congruence***
⇒ $a - b = np, p \in \mathbb{Z}$	***By definition of Divisibility***
⇒ $a - b + b =\ np + b$	***Add b to both sides of the Equation***
⇒ $a = np + b$	***LHS: Simplifying*** $-\boldsymbol{b} + \boldsymbol{b}$
⇒ $a + c = np + b + c$	***Add some integer c on both sides***

Since $n, p \in \mathbb{Z}$ therefore, $np \in \mathbb{Z}$ by ***Closure Property for Multiplication***. Also, since a, c, n, p therefore $a + c,\ np + b + c \in \mathbb{Z}$ by ***Closure Property for Addition.***

⇒ $(a + c) = np + (b + c)$	***By Associative Property for Addition***
⇒ $(a + c) + -(b + c) = np + (b + c)\ + -\ (b + c)$	***Add*** $-(\boldsymbol{b} + \boldsymbol{c})$ ***to both sides of the Equation***
⇒ $(a + c) - (b + c) = np$	***LHS: By definition of Subtraction*** ***RHS: Simplifying*** $(\boldsymbol{b} + \boldsymbol{c}) + -(\boldsymbol{b} + \boldsymbol{c})$
⇒ $n|(a + c) - (b + c)\ (mod\ n)$	***By definition of Divisibility***

End of Proof.

For (c.ii)

Proof.

Given: $a \equiv\ b\ (mod\ n)$

Need to Show: $ac \equiv\ bc\ (mod\ n)$

Suppose a, b, c, p ∈ ℤ, where $a \equiv b\ (mod\ n)$. Then it follows that:

• $a \equiv b\ (mod\ n)$	***Given***
⇒ $n\|(a - b)$	***By definition of Congruence***
⇒ $a - b = np, p \in \mathbb{Z}$	***By definition of Divisibility***
⇒ $(a - b)\ c = (np)\ c$	***Multiply some*** $\mathbf{c} \in \mathbb{Z}$ ***to both sides of the Equation***
⇒ $(a + -b)c = (np)\ c$	***LHS: By definition of Subtraction***
⇒ $ac + -\ bc = n\ (pc)$	***LHS: By Distributive Property for Multiplication over Addition*** ***RHS: By Associative Property Multiplication***

Since $a, b, c, p\ \in \mathbb{Z}$, therefore, $ac, bc, pc \in \mathbb{Z}$ by ***definition of Closure Property for Multiplication***. Also, since $-1, bc \in \mathbb{Z}$, therefore, $-1. bc = -bc \in \mathbb{Z}$ by ***Closure Property for Multiplication.***

⇒ $ac - bc = n\ (pc)$	***LHS: By Definition of Subtraction***

$\Rightarrow \quad n|(ac - bc)$ ***By Definition of Divisibility***

$\Rightarrow \quad ac \ = \ bc \ (mod \ n)$ ***By Definition of Congruence***

End of Proof.

For (c.iii)

Proof.

Given: a≡b (mod n)

Need to Show: $a^k \ \equiv b^k \ (mod \ n)$

Suppose $a, b, n \ \in \mathbb{Z}$ where $a \equiv \ b \ (mod \ n)$. Let $c \ = \ a^m$ and $d \ = \ b^m$ where $m \in W$ and $a^m \ b^m \ \in \mathbb{Z}$ such that $c \equiv \ \ d \ (mod \ n)$.

Then:

$\Rightarrow ac \equiv \ bd \ (mod \ n)$ ***By definition of Property (b.ii)***

$\Rightarrow a \ (a^m) \equiv b \ (b^m \ ) \ (mod \ n)$ ***Substituting the values of c and d***

$\Rightarrow a^{\ (1 \ + \ m)} \ \equiv b^{\ (1 \ + \ m)} \ (modn)$ ***Simplifying $\boldsymbol{a} \ (\boldsymbol{a^m})$ and $\boldsymbol{b} \ (\boldsymbol{b^m} \ )$***

By Law of Exponents

Since $1, m \in \mathbb{Z}$, therefore $1 + m \in \mathbb{Z}$ by ***Closure Property for Addition.***

$a^k \equiv b^k \ (mod \ n)$ ***Let $\boldsymbol{1 + m = k} \in \mathbb{Z}^+$***

End of proof.

A.2 CONGRUENCE CLASSES

Example: $n = 3$; $a = 13$; $b \ = 76$; $c = 5$; $a \ \equiv b \ (mod \ n)$

(i) $a + c\ \equiv\ b + d\ (mod\ n)$	***Property (c.i)***
$\Rightarrow 13 + 5 \equiv\ 76\ +\ 5\ (mod\ \ 3)$	***Substituting the values of a, b, c, n***
$\Rightarrow 18\ \ \equiv 81\ (mod\ \ 3)$	***Simplifying 13+5 and 76+5***
$\Rightarrow 3 \mid (18\ -\ 81)$	***By Definition of Congruence***
$\Rightarrow 3 \mid -63$	***Simplifying 18 - 81***
$\Rightarrow -63\ =\ 3\ (-21)$	***By Definition of Divisibility***

(ii) $a - c\ \equiv b - c\ (modn)$	***Property (c.i)***
$\Rightarrow 13 - 5\ \equiv 76 -\ 5\ (mod\ 3)$	***Substituting the values of a, b, c, n***
$\Rightarrow 8\ \equiv\ 71\ (mod\ 3)$	***Simplifying 13 - 5 and 76 - 5***
$\Rightarrow 3 \mid (8\ -\ 71)$	***By Definition of Congruence***
$\Rightarrow 3 \mid -63$	***Simplifying 8-71***
$\Rightarrow -63\ =\ 3\ (-21)$	***By Definition of Divisibility***

(iii) $a^2\ \equiv b^2\ (mod\ 3)$	***Property (c.iii)***
$\Rightarrow 13^2\ \equiv 76^2\ (mod\ 3)$	***Substituting the values of a, b, n***
$\Rightarrow 169 \equiv 5776(mod3)$	***Simplifying*** $\mathbf{13^2}$ ***and*** $\mathbf{76^2}$
$\Rightarrow 3 \mid 169 - 5776$	***By Definition of Congruence***
$\Rightarrow 3 \mid -5607$	***Simplifying 169-5776***
$\Rightarrow -5607\ =\ 3(-1,869)$	***By Definition of Divisibility***

Now, by Congruence Classes Modulo 3, we have:

Reflexive Property: → $1 \equiv 1 \ (mod\ 3)$

$2 \equiv 2 \ (mod\ 3)$

Remainder is 0: → $3 \equiv 0 \ (mod\ 3)$

$6 \ \equiv 0 \ (mod 3)$

Remainder is 1: → $4 \equiv 1 \ (mod\ 3)$

Remainder is 2: → $5 \equiv 2 \ (mod\ 3)$

$\boldsymbol{r = 1}: \ 1 \equiv 1 \ (mod\ 3) \qquad 4 \equiv 1 \ (mod\ 3) \qquad 7 \equiv 1 \ (mod\ 3)$

$\boldsymbol{r = 2}: \ 2 \equiv 2 \ (mod\ 3) \qquad 5 \equiv 2 \ (mod\ 3) \qquad 8 \equiv 2 \ (mod\ 3)$

$\boldsymbol{r = 3}: \ 3 \equiv 3 \ (mod\ 3) \qquad 6 \equiv 0 \ (mod\ 3) \qquad 9 \equiv 0 \ (mod\ 3)$

$\ldots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv \ldots \ (mod\ 3)$

$\ldots \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv 11 \equiv \ldots \ (mod\ 3)$

$\ldots \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv 12 \equiv \ldots \ (mod\ 3)$

A.3 APPLICATIONS ON CONGRUENCE:

(1) Show that $\mathbf{23}$ divides $\mathbf{2^{11} - 1}$

Solution:

Need to Show: $2^{11} \equiv (\ mod\ 23)$

Observe that : $2^5 \equiv 32 \equiv 9 \ (\ mod\ 23) \ \rightarrow \ 32 = 23(1) + 9$

So that:

$2^{11} \equiv 2^{10}.2 \ (\ mod\ 23)$ ***By Reflexive Property for Congruence***

$\Rightarrow 2^{11} \equiv (2^5)^2 \ (\ mod\ 23)$ ***Rewrite $\boldsymbol{2^{10} as}\ (\mathbf{2^5})^{\mathbf{2}}$ by Law of Exponent***

$\Rightarrow 2^{11} \equiv (9)^2 . 2 \ (mod\ 23)$	***By Congruence Classes or Transitive Property for Congruence***
$\Rightarrow 2^{11} \equiv 81.2 \ (mod\ 23)$	***Simplifying*** $\mathbf{9^2}$
$\Rightarrow 2^{11} \equiv 12.2 \ (mod\ 23)$	***Transitive Properly for Congruence*** 92^{11}
$\Rightarrow 2^{11} \equiv 24 \ (mod\ 23)$	***Simplifying*** $\mathbf{12.2}$
$\Rightarrow 2^{11} \equiv 1 \ (mod\ 23)$	***By Transitive Property for Congruence***
$\Rightarrow 2^{11} + -1 \ \equiv 1 + \ -1 \ (mod\ 23)$	***By Property (c.1) of Congruence***
$\Rightarrow 2^{11} - 1 \equiv 0 \ (mod\ 23)$	***LHS: By Definition of Subtraction*** ***RHS: Simplifying*** $\mathbf{1 - 1}$
$\Rightarrow 23 \vert (2^{11} - 1)$	***By Definition of Congruence***

(2) What is the remainder when $\mathbf{2^{67}}$ divided by 7?

Solution:

Observe that $2^3 = 8 \equiv 1 \ (mod\ 7)$. Then, we have

$\Rightarrow 2^{67} \equiv 2^{66} . 2 \ (mod\ 7)$	***By Reflexive Property for Congruence***
$\Rightarrow 2^{67} \equiv (2^3)^{22} \ .2 \ (mod\ 7)$	***Rewrite*** $\mathbf{2^{66}}$ ***as*** $\mathbf{(2^3)^{22}}$ ***by Law of Exponent***
$\Rightarrow 2^{67} \equiv (8)^{22} \ .2 \ (mod\ 7)$	***Simplifying*** $\mathbf{(2^3)}$
$\Rightarrow 2^{67} \equiv (1)^{22} \ .2 \ (mod\ 7)$	***By Transitive Property for Congruence***
$\Rightarrow 2^{67} \equiv 1.2 \ (mod\ 7)$	***Simplifying*** $\mathbf{(1)^{22}}$
$\Rightarrow 2^{67} \equiv 2 \ (mod\ 7)$	***Simplifying*** $\mathbf{1.2}$

Therefore, r=2 when $\mathbf{2^{67}}$ ***is divided by 7.***

(3) Find the units digit of $\mathbf{13^{79}}$

Solution: Observe that $13^2 \equiv 169 \equiv 9\ (mod\ 10)$.

Then, we have:

$\Rightarrow 13^{79} \equiv 13^{78}.13\ (mod\ 10)$	***By Reflexive Property for Congruence***
$\Rightarrow 13^{79} \equiv (13^2)^{39}.13\ (mod\ 10)$	***Rewrite as*** $\mathbf{13^{78}}$ ***as*** $(\mathbf{13^2})^{\mathbf{39}}$
	By Law of Exponent
$\Rightarrow 13^{79} \equiv (9)^{39}.13\ (mod\ 10)$	***Transitive Property For Congruence***
$\Rightarrow 13^{79} \equiv (-1)^{39}.13\ (mod\ 10)$	***By Congruence Classes Modulo 10***
	$\mathbf{...\equiv 19 \equiv 9 \equiv -1 \equiv ...(\mathit{mod}\ 10)}$
$\Rightarrow 13^{79} \equiv -1.13\ (mod\ 10)$	***Simplifying*** $(\mathbf{-1})^{\mathbf{39}}$
$\Rightarrow 13^{79} \equiv -13\ (mod\ 10)$	***Simplifying*** $\mathbf{-1.13}$
$\Rightarrow 13^{79} \equiv -3\ (mod\ 10)$	***By Congruence Classes Modulo 10***
	$\mathbf{...\equiv 23 \equiv -13 \equiv -3 \equiv ...(\mathit{mod}\ 10)}$
$\Rightarrow 13^{79} \equiv 7\ (mod 10)$	***By Congruence Classes Modulo 10***
	$\mathbf{...\equiv -13 \equiv -3 \equiv 7 \equiv ...(\mathit{mod}\ 10)}$

Therefore, the unit digit of $\mathbf{13^{79}}$ ***is*** **7.**

(4) Find the remainder obtained upon dividing the sum $(\mathbf{1! + 2! + ... + 100!})$ by 12.

Solution:

Observe that $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24 \equiv 0\ (mod\ 12)$. Also,

$5! = 5.4!$. So that:

$\Rightarrow 5! \equiv 5.4!\ (mod\ 12)$ ***By Reflexive Property for Congruence***

$\Rightarrow 5! \equiv 5.0\ (mod\ 12)$ ***By Transitive Property for Congruence***

$\Rightarrow 5! \equiv 0\ (mod\ 12)$ ***Simplifying 5.0***

- $100! \equiv (100\,.99\ldots.5)\,.4!\,(mod\ \ 12)$ ***By Reflexive Property for Congruence***
- $100! \equiv (100.99\ldots..5).0\ (mod\ 12)$ ***Transitive Property For Congruence***
- $100! \equiv 0\ (mod\ 12)$ ***Simplifying*** $\mathbf{(100.99\ldots..5).0}$

Also, observe that:

- $1! \equiv 1\ (mod\ 12)$ ***By Reflexive Property for Congruence***
- $2! \equiv 2\ (mod\ 12)$ ***By Reflexive Property for Congruence***

$3! \equiv 6\ (mod\ 12)$ ***By Reflexive Property for Congruence***

Therefore, $\mathbf{1! + 2! + 3! + 4! + \ldots + 100! \equiv 1 + 2 + 6 + 0 + \ldots + 0\ (mod\ 12)}$ ***By Transitive Properly For Congruence***

$1! + 2! + 3! + 4! + \ldots + 100!\ \ \equiv 9\ (mod\ 12)$ ***Simplifying*** $\mathbf{1 + 2 + 6 + 0 + \ldots + 0}$

Thus, the remainder obtained upon dividing the sum $1! + 2! + 3! + 4! + \ldots + 100!$ by 12 is 197.

(5) What is the last digit in the sum $\mathbf{3^{17} + 7^{13}}$?

Solution:

For 3^7observe that $3^2 = 9 \equiv -1\ (mod\ 10)$.

So that:

$\Rightarrow 3^{17} \equiv 3^{16}.3\ (mod 10)$ ***By Reflexive Property for Congruence***

$\Rightarrow 3^{17} \equiv (3^2)^8.3\ (mod 10)$ ***Rewriting*** $\mathbf{3^{16}\ \ (3^2)^8}$ ***by Law of Exponent***

$\Rightarrow 3^{17} \equiv\ (9)^8.3\ (mod 10)$ ***Simplifying*** $\mathbf{3^2}$

$\Rightarrow 3^{17} \equiv (-1)^8 . 3\ (mod 10)$ ***By Transitive Property for Congruence***

$\Rightarrow 3^{17} \equiv 1.3\ (mod 10)$ ***Simplifying*** $(-\mathbf{1})^{\mathbf{8}}$

Therefore, the last digit of $\mathbf{3^{17}}$ ***is 3***

For 7^{13} observe that $7^2 = 49 \equiv 9(mod\ 10)$.

So that:

$7^{13} \equiv 7^{12}. 7$ (mod 10) ***By Reflexive Property For Congruence***

$\Rightarrow 7^{13} \equiv (7^2)^6 . 7$ (mod 10) ***Rewrite*** $\mathbf{7^{12}}$ ***and*** $(\mathbf{7^2})^{\mathbf{6}}$***by Law of Exponent***

$\Rightarrow 7^{13} \equiv (49)^6 . 7$ (mod 10) ***Simplifying*** $(\mathbf{7^2})$

$\Rightarrow 7^{13} \equiv (9)^6 . 7$ (mod 10) ***By Transitive Property for Congruence***

$\Rightarrow 7^{13} \equiv (-1)^6 . 7$ (mod 10) ***By Congruence Classes Modulo 10***

$\ldots \equiv \mathbf{19} \equiv \mathbf{9} \equiv -\mathbf{1} \equiv . . . (\mathbf{mod\ 10})$

$\Rightarrow 7^{13} \equiv 1.7$ (mod 10) ***Simplifying*** $(-\mathbf{1})^{\mathbf{6}}$

$\Rightarrow 7^{13} \equiv 7$ (mod 10) ***Simplifying*** $\mathbf{1.7}$

Therefore, the last digit of $\mathbf{7^{13}}$ ***is 7.***

Thus, we have:

$\Rightarrow 3^{17} + 7^{13} \equiv 3 + 7\ (mod\ 10)$ ***By Transitive Properly for Congruence***

$\Rightarrow 3^{17} + 7^{13} \equiv 10\ (mod\ 10)$ ***Simplifying*** $\mathbf{3 + 7}$

$\Rightarrow 3^{17} + 7^{13} \equiv 0\ (mod\ 10)$ ***By Congruence Classes Modulo 10***

$\ldots \equiv \mathbf{20} \equiv \mathbf{10} \equiv \mathbf{0} \equiv . . . (\boldsymbol{mod}\mathbf{10})$

The last digit of the sum of $\mathbf{3^{17} + 7^{13}}$ ***is*** $\mathbf{0}$.